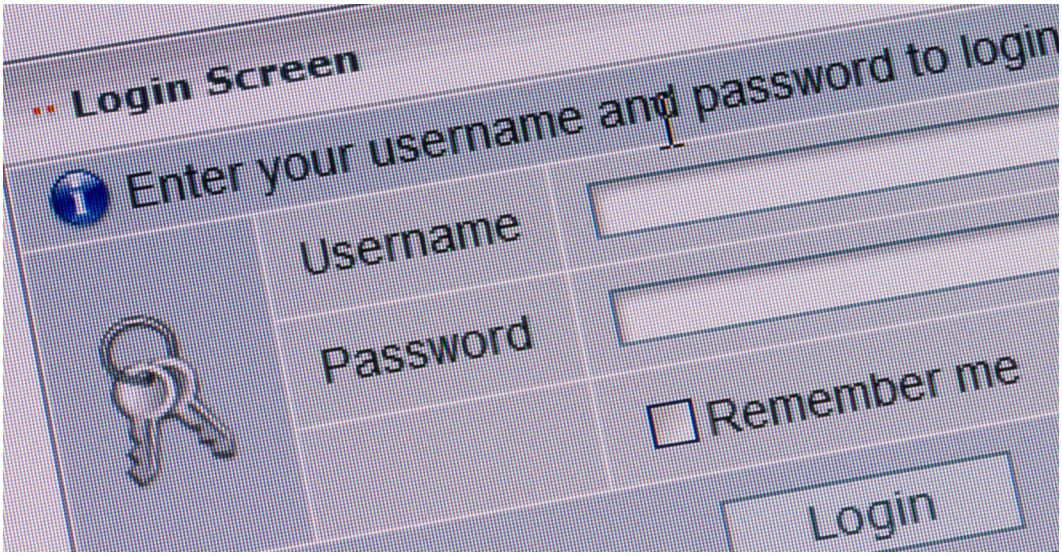
Summer 2011
Volume 2, Issue 2

Published quarterly by DoD PKE

The PKE *Quarterly Post*

New DoD Authentication Policy



In May 2011, *DoD Instruction (DoDI) 8520.2: Public Key Infrastructure (PKI) and Public Key (PK) Enabling,* was superseded by two new documents, *DoDI 8520.02: Public Key Infrastructure (PKI) and Public Key (PK) Enabling* [1], and *DoDI 8520.03: Identity Authentication for Information Systems* [2]. These new policy documents govern all DoD information systems and introduce significant changes to the requirements for public key enabling networks, web servers, and other information systems.

The new DoDI 8520.02 is primarily a re-release of DoDI 8520.2 that establishes the availability of the Coalition PKI for Combatant Commands (COCOMS), refers to the SIPRNET PKI that will be transitioned to operate under Committee for National Security Systems (CNSS) authority, provides specific guidance on issuance of alternate (ALT) tokens to Flag-level officers or Senior Executives, and incorporates the DoD CIO "Approval of External PKIs" memorandum (circa July 2008) into the instruction. It also contains two other major changes. The first is that all policy related to authentication requirements has been moved to DoDI 8520.03. The second major change impacts pursuing waivers to DoDI 8520.02. Previously, Component CIOs had the authority to approve waivers to the instruction. Under the new policies, Component CIOs must endorse waivers, but all waiver requests must be submitted to the Defense Information System Network/Global Information Grid (DISN/GIG) Flag Panel for approval.

1 http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf
2 http://www.dtic.mil/whs/directives/corres/pdf/852003p.pdf

continued on page 3

In This Issue

In Every Issue

Ask the Expert

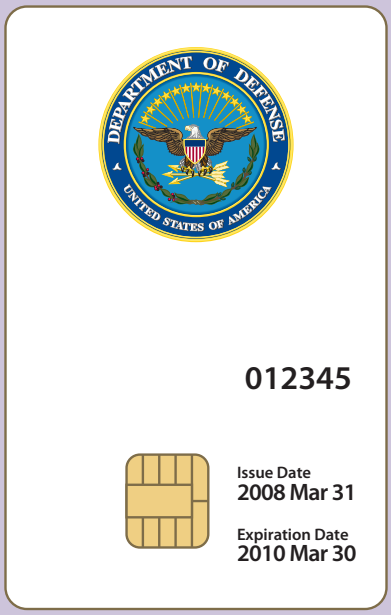
How do I get the DoD Root CA thumbprint?

In order to ensure the authenticity of the DoD Root CA 2 certificate before trusting or installing the certificate on a system, the SHA-1 hash of the certificate should be verified. Verification of the hash consists of comparing a local hash of the certificate to a trusted provider's record of the hash.

The first step is to view the SHA-1 hash or thumbprint of the local copy of the DoD Root CA 2 certificate in question. On a Windows system, the SHA-1 hash can be viewed by opening the DoD Root CA 2 certificate file, clicking on the details tab and scrolling down to the last field labeled "Thumbprint." Alternatively, OpenSSL can be used to display the SHA-1 hash of the DoD Root CA 2 certificate by running the following command from the directory containing the certificate:

openssl x509 –in *<DoD Root CA 2 filename>* –fingerprint –noout

The second step is to verify the thumbprint obtained in the first step with the DoD PKI Help Desk. The help desk can be reached at (800) 490-1643 or DSN 339-5600. Ask the DoD PKI Help Desk representative to provide the DoD Root CA 2 SHA-1 thumbprint and ensure it matches exactly the thumbprint from the first step to validate the authenticity of the certificate.



What is an Alternate Logon Token (ALT)?

The Alternate Logon Token (ALT) is a smart card containing a certificate issued from the DoD PKI to provide logical access to DoD networks and systems. The exterior of the ALT contains an image of the DoD seal, but no identifiable information of the ALT holder. A typical use case of an ALT is to enable separation of duties for a system administrator by offering a secondary smart card linked to a privileged account, while the system administrator's CAC is linked to his or her user account. This offers the DoD a secure two-factor method for logically authenticating to multiple accounts. The process to obtain an ALT can vary by CC/S/A, so users interested in ALTs should contact their Local Registration Authority (LRA) or Registration Authority (RA) for the specific steps to obtain an ALT.

What is the difference between the DoD ECA PKI and DoD-Approved External PKIs?

The DoD External Certification Authority (ECA) program is sponsored by the DoD to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations who have a need to interoperate with the DoD but do not have access to DoD or other approved PKI credentials. The DoD developed the Certificate Policy (CP) governing the ECA PKI, and ECA Root CAs are managed by the Defense Information Systems Agency (DISA), with subordinate CAs operated by ECA vendors under agreement with the DoD. ECA PKI certificates are available to the public for purchase from the designated ECA vendors.

DoD-approved external PKIs are typically managed by distinct DoD partner organizations, such as other federal agencies or industry, to serve their own employees or other specific populations. Each external PKI operates their own infrastructure in accordance with a CP which has been determined to comply with the requirements defined in the Federal Bridge Certification Authority (FBCA) CP, and has a cross-certificate relationship with the Federal Bridge that defines relative assurance levels of its certificates. Approved external PKIs are not DoD-sponsored or operated, but are approved for use by DoD relying parties.

For more information, visit the DoD PKE web site at **http://iase.disa.mil/pki-pke** and click on Interoperability.

Notes from DoD PKE

With the conference season now behind us, it has remained a busy time for the DoD PKE team. We want to thank all of the CC/S/As and attendees for your valuable contributions to the PKE track at the 2011 Identity Protection and Management Conference (IPMC). Without you, success would not have been possible. Exciting topics briefed at the IPMC included Trust Store Management, Java and PKE, Authorization and Authentication for Web Servers, and State of Commercial Mobile Devices in the DoD, just to list a few. All briefings and presentations from the PKE track are available on the DoD PKE web site at **http://iase.disa.mil/pki-pke** under Conferences.

Speaking of the PKE website, if you have visited recently you may have noticed we've made some big changes to improve the site's usability. Among these changes is the PKE A-Z page which provides all of our documents and tools in one location to make searching for what you need easier. Document and tool titles have also been standardized to use a new naming convention. See the DoD PKE Web Site Refresh article on page 5 for more details.

InstallRoot is now publicly available on the Tools page. Please check out the Ask the Expert column to learn more about how to get and verify the DoD Root CA thumbprint once InstallRoot is obtained. The DoD PKE team will also be providing signed PKCS#7 files containing the same certificates available via InstallRoot during the next release. These files will provide a method for non-Windows operating systems to obtain the DoD PKI certificates. For more information read the In the Pipeline item on page 3 or just visit our site!

This newsletter's cover story focuses on the recent policy instructions released by ASD(NII)/DoD CIO. These new policy requirements introduce significant changes to how DoD pk-enables networks, web servers, and other information systems. In a nutshell, *DoD Instruction 8520.2: Public Key Infrastructure (PKI) and Public Key (PK) Enabling,* has now been superseded by two new instructions, DoDI 8520.02 and DoDI 8520.03. The cover story explains the differences between these instructions, major changes, and a high level comparison of requirements between the old DoDI 8520.2 and the new DoDI 8520.03.

A new and fun edition to the PKE Quarterly is the PKE Puzzle Corner. Try your hand at deciphering this issue's cryptogram. The solution will be available in the fall edition of the newsletter and under the Newsletters section of the DoD PKE website.

New DoD Authentication Policy – *continued*

DoDI 8520.03 requires that all authentications of users be conducted with an appropriate credential that is approved for use by DoD authority and has been verified as active (not revoked) and not expired by the credential issuing authority. Appropriate credentials should be identified and designated by information system owners by looking at the following three dimensions:

- The sensitivity of the information being accessed
- The environment from which the user is authenticating to the DoD information system
- The strength of the credential being used for the authentication

DoDD 8500.1 defines sensitive information as distinct from public or classified information. DoDI 8520.03 defines four levels of data sensitivity granularity for sensitive but unclassified information, and three levels of data sensitivity granularity for Secret or Confidential information. It then provides specific requirements for authentication credentials based on these levels of sensitivity.

The following table provides a high level comparison of requirements between the old DoDI 8520.2 and the new DoDI 8520.03.

#	Authentication	DoDI 8520.2	DoDI 8520.03
1	Approved for public release	No authentication required	No authentication required
2	Network logon	PKI authentication required (NIPRNET and SIPRNET) using a DoD PKI hardware token certificate	PKI authentication required (NIPRNET and SIPRNET) using a PIV credential or other credential specifically approved by the CIO (e.g. Alternate Tokens for system administrators working in Windows Server 2003 domains)
3	Web server authentication	PKI authentication required (NIPRNET and SIPRNET) using a certificate issued by the DoD PKI or a DoD Approved External PKI. Exception is made for personal information for information privileged individuals who can use minimum of username/password	Data owner must determine sensitivity level of information. Instruction defines four sensitivity levels for NIPRNET and three sensitivity levels for SIPRNET, along with specific requirements for administrator logon. • Level 1 (NIPRNET): Username/password acceptable • Level 2 (NIPRNET): Non-PKI multi-factor except: – When user is authenticating to a system from unmanaged device, hardware PKI certificate from a DoD PKI or DoD Approved External PKI is required – When both user and system are on a DoD network, username/password is acceptable • Level 3 (NIPRNET): Software PKI certificate issued by the DoD PKI or a DoD Approved External PKI except: – When user is accessing system from unmanaged device, hardware PKI certificate from a DoD PKI or DoD Approved External PKI is required – When both user and system are on a DoD network, a non-PKI multi-factor credential is acceptable • Level 4 (NIPRNET): PKI authentication required using a PIV credential or credential specifically approved • Level 5 (SIPRNET): Username/password acceptable • Level 6 (SIPRNET): Software PKI certificate issued by the NSS PKI, cross certified by the NSS PKI, or approved by DoD • Level 7 (SIPRNET): Hardware PKI certificate issued by the NSS PKI, cross certified by the NSS PKI, or approved by DoD
4	Other information system authentication	PKI authentication required only if warranted	No special requirements, requirements are the same as those in row 3 for web server authentication.

Based on this policy change, information system owners should evaluate the types of information that can be accessed from the system, determine the sensitivity level that correlates to their system's information and decide which of their user populations will be requesting access to the information. To determine the credential types that should be supported for authentication use the table provided in DoDI 8520.03. If the information system can determine the user's computer and/or network environment, lesser assurance credentials may be acceptable for some sensitivity levels. If the information system cannot determine the user environment, the system must assume the user is coming from an untrusted environment or direct users to authenticate to the system from a specified environment and set credential strength requirement accordingly.

In the Pipeline

Signed PKCS#7 Files for Non-Windows Products

DoD PKE will begin hosting digitally signed PKCS#7 files containing the same certificates available via our various versions of InstallRoot. These new files will provide a trusted distribution method for obtaining and consuming DoD PKI and related certificates on non-Windows operating systems or with non-Windows products. They can also serve as an alternate method for certificate distribution to Windows-based products for organizations that may prefer using a PKCS#7 format over the traditional InstallRoot distribution. The new files will be hosted on the DoD PKE web site in the same locations from which InstallRoot is currently available.

External Certification Authority (ECA) 1024-bit Root to be Retired

In July 2011, the last end user certificates issued from Certification Authorities (CAs) under the 1024-bit ECA Root CA expired. Although some of the subordinate CAs are still valid, it is recommended that DoD relying parties who accept ECA certificates remove the 1024-bit ECA Root CA and its subordinate CAs from their trust stores, and ensure that the current 2048-bit ECA Root CA 2 and its subordinates, which serve the current ECA user population, are trusted. The thumbprint of the soon-to-be-decommissioned root is included below for reference.

1024-bit ECA Root CA thumbprint:
3a 32 ef 7b 9a b8 36 f8 37 18 1a 4c ef a3 55 c6 46 67 ac bf

continued on page 5

RA/LRA/KRA Corner

RA Workstation Configuration Recommendations for Windows Vista and 7

In response to requests from the community, the PKI PMO is in the process of developing recommended Registration Authority (RA) workstation configuration steps to best equip Windows Vista and 7 machines to comply with RA audit requirements set forth in the DoD PKI Reference Certification Practice Statement (CPS). The recommendations will include steps for user account configuration, access control, virus scanning, security event log configuration, restriction of available services and applications, and network security requirements. The document is planned for release this fall.

RA/LRA/KRA Contact Information

RA Operations			
Name	**Organization**	**Contact Information**	**COCOMs Support**
Army	Army CTNOSC Army NETCOM	ctnosc.pki@us.army.mil (Equipment Certificates) army.ra@us.army.mil (User Certificates)	USEUCOM USSOUTHCOM USAFRICOM
Air Force	Air Force PKI Help Desk	https://afpki.lackland.af.mil/html/lracontacts.asp (Local Registration Authority Base Contacts) afpki.ra@us.af.mil	USCENTCOM USSOCOM USTRANSCOM USNORTHCOM USSTRATCOM
Navy	Navy PKI Help Desk	https://infosec.navy.mil/PKI/lramain.html	USJFCOM USPACOM
Marine Corps	USMC PKI RA Operations	raoperations@mcnosc.usmc.mil	Not an Executive Agent
Joint Staff	Joint Staff RA Support Help Desk	jsra@js.pentagon.mil	Not an Executive Agent
DLA	DLA RA Operations	dlapki@dla.mil	Not an Executive Agent
DISA	DISA RA Operations	disaraoperations@disa.mil	Not an Executive Agent
WHS	WHS IPM Team	whsra@whs.mil	Not an Executive Agent

Permanent Identifier in Software Certificates

When the DoD PKI was originally deployed, all certificates were in software. The certificate common name (CN) consisted of the individual's name and a ten-digit unique identifier obtained from a block of numbers assigned to each Local Registration Authority (LRA). Each time a user got a new certificate, he received a new ten-digit identifier.

When the PKI began issuing Common Access Cards (CACs), that ten-digit number became permanently linked to a specific user and known as the Electronic Data Interchange Personal Identifier (EDIPI). A big advantage of permanent identifiers is that applications don't necessarily have to reregister users when they get new certificates (depending on how they map certificates into user accounts).

For many years, permanent identifiers were only in CAC certificates and not in software certificates. A few years ago, it became possible to issue software certificates with the same EDIPI found in CACs. Now, as long as a user has a record in the Defense Enrollment Eligibility Reporting System (DEERS) and the LRA uses the LRA thin client interface, the user will receive a software certificate with his EDIPI.

JPAS Transitioning to Certificate-Based Authentication

The Joint Personnel Adjudication System (JPAS) logon procedures are being updated to provide additional security and privacy of clearance data and personally identifiable information (PII).

Traditionally, access to JPAS was with a user ID and password; however, starting in August 2011 users can access JPAS with a valid JPAS account and one of the following PKI credentials:

1. DoD Common Access Card (CAC)
2. Federal Agency Personal Identity Verification (PIV) Card
3. External Certification Authority (ECA) PKI medium-token or medium hardware assurance certificate
4. Other DoD-approved PKI certificate that is cross-certified with the Federal Bridge at medium hardware assurance or higher

Users who do not have or qualify for a DoD CAC, PIV card, or other organization-specific approved external PKI certificates can apply for ECA medium-token or medium hardware certificates.

continued on page 6

Wireless Update

This edition discusses the DoD Chief Information Officer (CIO) commercial mobile devices (CMD) memo released in April 2011 and the DoD PKE team's experience with the Biometrics Associates, LP (BAL) baiMobile 3000MP Bluetooth smart card reader (SCR) for iOS and Android.

DoD CIO CMD Memo

The DoD CIO released a memo on April 6th, 2011 entitled, "Use of Commercial Mobile Devices (CMD) in the Department of Defense (DoD)." The memo emphasized the importance of adhering to existing security policies when considering the use of CMDs such as smartphones, e-readers, and tablets. The CMD memo also identified significant requirements, provided potential mitigations for limited use pilots and mission critical applications, and requested that copies of supporting accreditation documentation and/or best practices be sent to the CMD Working Group (CMDWG) for community sharing. A PKI requirement included in the memo stated, "Devices must implement DoD PKI Standards or approved authentication credentials."

BAL baiMobile 3000MP

Good Technology, the vendor providing the Good for Enterprise security overlay required in the current drafts of both the iOS and Android Security Technical Implementation Guides (STIG), worked with BAL to bring a Bluetooth SCR to both mobile platforms. The iOS platform requires the use of a baiMobile Bluetooth Adapter plugged into the data/power port of the iOS device. The baiMobile 3000MP Bluetooth SCR (along with the iOS adapter) recently completed a Bluetooth Security evaluation by Spanalytics, LLC. The solution helps enable secure mobile collaboration and information sharing capabilities using iOS- and Android-based CMDs. The Good Technology Good For Enterprise solution leverages the baiMobile 3000MP to utilize DoD-approved PKI credentials [e.g., certificates on the Common Access Card (CAC)]. More information about the baiMobile 3000MP can be found at http://www.biometricassociates.com/products-baimobile/smart-card-reader-iphone-android.html.

Test Performance

DoD PKE performed initial testing of the PKI capabilities of the baiMobile 3000MP SCR with Good Technology's Good for Enterprise solution. Overall, email capabilities were found to be good, while certificate-based authentication capabilities were lacking. In email testing, sending signed and encrypted Secure/Multipurpose Internet Mail Extension (S/MIME) messages and receiving/decrypting encrypted S/MIME messages worked as expected using a smart card. The main negative experience revolved around the Bluetooth pairing process; the user is not currently given much feedback during the pairing process, and it can seem like the pairing completed successfully when it actually did not. The Good for Enterprise solution did not support certificate-based authentication to the device, to web sites via the device browser, or to the email server at the time of testing.

Due to the rapid development cycle of the Good Technology solution, the product is constantly being changed and improved, so as the product matures and development time stabilizes, additional PKI-related testing using the baiMobile 3000MP will need to be performed.

Neither the iOS nor Android platforms have yet been approved for use in the DoD. Organizations interested in piloting the devices should refer to the DoD CIO CMD memo for information about setting up a pilot.

DoD PKE Web Site Refresh

If you've visited the DoD PKE team's web site at http://iase.disa.mil/pki-pke recently, you may have noticed some changes. In February we decommissioned our Defense Knowledge Online (DKO) site and consolidated our web presence on DISA's Information Assurance Support Environment (IASE) portal. The team has been working to improve the IASE site's usability by making information easier to find. Notable updates include:

- **PKE A-Z page**—The new PKE A-Z page provides one-stop shopping for all materials available on the site.
- **Tools page**—The new Tools page replaces the old Most Requested Downloads page, and contains all of the Tools (and their corresponding documentation) maintained by DoD PKE.
- **Document naming convention updates and descriptions**—Document names listed on the site have been standardized to use a [Product]: [Activity] naming convention; for example, the old RG: Key Store Tools & Procedures is now Keytool, CertUtil and OpenSSL: Common Certificate Procedures. A short description of each item's contents and purpose is also included with the listing.
- **Content presentation refresh**—Materials are now listed alphabetically in topical tables. Each table row displays the title of the document or tool, and can be expanded to view the item's description. Linked listings of table categories are available at the top of each page to allow you to quickly jump to the table(s) relevant to your search.

continued on page 7

In The Pipeline - *continued*

SIPRNet RCVS DTM Migration

The first SIPRNet RCVS node is scheduled to be migrated to the Delegated Trust Model (DTM) on September 19th, 2011, with the second node being migrated on October 18th, 2011. During the bridge period between the two nodes' migration, SIPRNet RCVS will be operating in a mixed mode. OCSP clients which submit requests to the standard load-balanced RCVS SIPRNet URL may receive responses in either the current Explicit (self-signed) Trust Model from the unmigrated node, or in DTM from the migrated node. At completion of the second node's migration, all relying parties must be able to validate an OCSP response using a DTM certificate. You can find more information on the different OCSP trust models in the OCSP slick sheet on the A-Z page of the DoD PKE web site at http://iase.disa.mil/pki-pke.

Latest Tool Releases

These tools are available from the DoD PKE site at http://iase.disa.mil/pki-pke under Tools unless otherwise noted.

DownloadCRL 2.2 for Linux: This release of DownloadCRL has been updated to support Global Directory Service (GDS) 2.0 URLs and leverage static certificate revocation list (CRL) distribution points. Permissions requirements have been modified to allow users without home directories (such as service accounts) to execute the program, and error handling has been refined.

InstallRoot-J 3.15: This release includes new Joint Interoperability Test Command (JITC) PKI test identity and email CAs 27-30 as well as test SHA-256 identity and email CAs.

InstallRoot-E 3.15: This release includes three new External Certification Authority (ECA) subordinate CAs: ORC ECA SW 4, ORC ECA HW 4, and VeriSign Client External Certification Authority - G3. It no longer includes the 1024-bit ECA Root CA and its subordinates since all end entity CAs issued off of that infrastructure have expired (see In the Pipeline item).

PKI Interoperability Test Tool (PITT) 1.2.5: This release includes updated signature verification logic to correct a bug related to linked certificates processing. The tool is available on SourceForge at http://pkif.sourceforge.net/pitt.html.

Federal Bridge 2.0

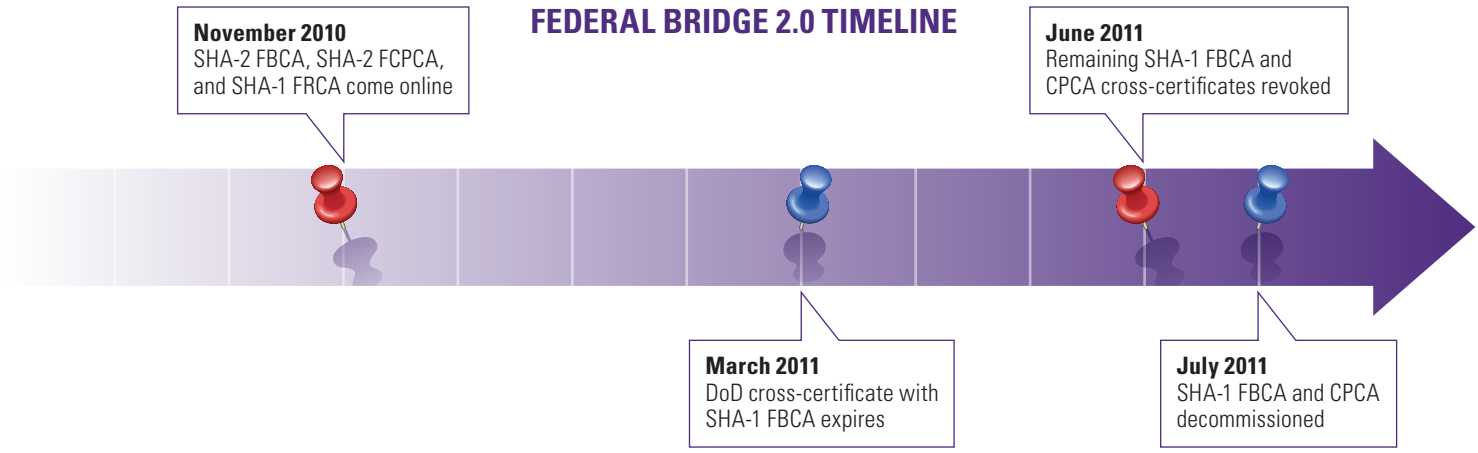
The federal government's migration to the use of Secure Hash Algorithm (SHA)-256 in their Public Key Infrastructures (PKI) in accordance with the National Institute of Standards and Technology (NIST) timelines set forth in Special Publications (SP) 800-57 and 800-131A has necessitated updates to the landscape of the Federal Bridge to accommodate the migration.

A year ago, the keystone of the Federal Bridge was the SHA-1-based Federal Bridge Certification Authority (FBCA), with which federal agency and partner PKIs cross-certified in order to interoperate using cross-certificate trust. In concert with the FBCA, the General Services Administration (GSA) operated the Common Policy Certification Authority (CA) with shared service provider (SSP) subordinate CAs to serve agencies that did not operate their own PKIs.

In November 2010, the Federal PKI Management Authority (FPKIMA) deployed a new infrastructure to support both federal agencies migrating to SHA-256 by the January 1, 2011 NIST deadline and those agencies (such as DoD) which delayed migration and continued to operate using SHA-1 under the acceptance-of-risk condition set forth in NIST SP 800-131A. The new infrastructure includes:

Over the months following the deployment of the new Federal PKI, the FPKIMA moved forward with decommissioning the legacy FBCA and Common Policy CA, first revoking any still-valid cross-certificates, and finally decommissioning the systems in July 2011.

For DoD users, the changes to the Federal Bridge infrastructure should be largely transparent, with a few exceptions. Anyone looking at issuance chains for partners still using SHA-1 may notice that the chain now includes the FRCA rather than the FBCA. DoD organizations using an old version of the FBCA Cross-Certificate Remover tool may also have seen a recurrent of the Microsoft cross-certificate chaining issue, and need to run the latest version of the tool (1.06 at the time of publication) to establish a permanent fix for the current infrastructure. Finally, although not strictly related to the Federal Bridge infrastructure, any organizations that are directly trusting federal partners rather than leveraging the bridge infrastructure may need to update their trust stores to trust SHA-256 roots that other agencies and partners have brought online as part of their migration efforts. Updated trust anchors are available on the DoD PKE IASE at http://iase.disa.mil/pki-pke under the Interoperability link.



Federal Bridge Certification Authority: The new SHA-256-based FBCA with which SHA-2 federal and partner PKIs cross-certify. Subject OU = Entrust, OU = FBCA, O = U.S. Government, C = US.

Federal Common Policy Certification Authority (FCPCA): The new GSA-operated Common Policy root serving most agencies without their own PKIs; also cross-certifies some federal legacy PKIs. Subject OU = Entrust Managed Services Root CA, OU = Certification Authorities, O = Entrust, C = US.

SHA-1 Federal Root Certification Authority (FRCA): The replacement for the SHA-1 FBCA, against which all SHA-1 federal and partner PKIs cross-certify. Subject CN = SHA-1 Federal Root CA, OU = FPKI, O = U.S. Government, C = US.

The DoD PKI's relationship to the Federal Bridge is in accordance with the general descriptions of the new infrastructure components' roles listed above. Since DoD is still issuing SHA-1 PKI certificates, our cross-certificate relationship between the DoD Interoperability Root CA (IRCA) and the legacy FBCA which expired prior that CA's decommissioning was replaced by a cross-certificate with the FRCA. In the coming months, DoD will be deploying IRCA 2, which will be cross-certified with the new SHA-256 FBCA and will serve as the SHA-256 corollary to our current SHA-1 IRCA (which is cross-certified with the SHA-1 FRCA). IRCA 2 will allow DoD to smoothly transition to interoperating with the federal community via the SHA-256 FBCA once the DoD PKI begins issuing SHA-256 signed certificates.

JPAS Transitioning – *continued*

The ECA program is managed by the Defense Information Systems Agency (DISA) and is intended to provide contractors and civilians who do not qualify for CACs the ability to obtain PKI certificates so they can do business with the DoD. Information about obtaining an ECA certificate can be found at http://iase.disa.mil/pki/eca.

Users will be able to continue using user IDs and passwords for authenticating to JPAS until January 2012, when the Defense Manpower Data Center (DMDC) will remove this authentication option.

Additional Information can be found on the DMDC web site at https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS. Select JPAS PKI FAQs from the left navigation menu.

In June, we also decommissioned the DKO External Interoperability site and migrated its contents to an Interoperability sub-site on the DoD PKE IASE site. On the Interoperability main page (accessed by clicking the Interoperability link from the DoD PKE home page), you'll find a list of all of the currently approved external PKIs and the partners each serves. Clicking on any approved PKI will take you to a page containing that PKI's Certification Authority (CA) certificates, CA certificate information including thumbprints for verification, and approved policy object identifiers (OID) to assist in the implementation of assurance level filtering for direct trust deployments. You'll also find other external interoperability-related materials on the Interoperability main page, such as the DoD External Interoperability Plan which details who can become a DoD-approved PKI and how, and the Joint Interoperability Test Command (JITC) interoperability test plans for external PKIs as well as applications.

Air Force Offline Certificate Request Tool

The Air Force (AF) Public Key Infrastructure (PKI) System Program Office (SPO) developed an Offline Device Certificate Request Tool to enable generation of certificate requests for both DoD and AF PKI certificates. The Offline Device Certificate Request Tool can be run directly on the Microsoft server host that requires the certificate, or on a Microsoft machine other than the target host to generate an offline request for the target host. In the latter case, the target host system must be able to accept a PKCS#12 certificate file import. Once the request has been generated and saved on the requesting machine, system administrators must submit the request to one of the DoD device certificate issuing CAs and complete the necessary paperwork with their Local Registration Authority (LRA) to have the request validated and approved by their Service Registration Authority (RA).

Currently the published version of the tool on the AF PKI SPO web site only supports requests generated on Windows Server 2003 and Windows XP workstations. Windows Server 2008 systems being deployed as Domain Controllers (DC) can use the innate capabilities of the operating system to generate DC certificate requests following the instructions at https://afpki.lackland.af.mil/assets/files/OE-11-07-010-Server_2008_DC_Cert_Request_Procedures_v1000.pdf.

The Offline Certificate Request Tool is available to any system administrator within DoD and is accessible from the AF PKI SPO web site at https://afpki.lackland.af.mil/html/offlinedev-certs.cfm. The site is restricted to .mil domain access only.

About DoD PKE

The DoD Public Key Enabling (PKE) Team is chartered with helping DoD customers leverage existing and emerging PKI capabilities for increased productivity and an improved Information Assurance posture. We provide engineering consultations, develop enterprise solutions, create collaboration environments, and work to make commercial products interoperate with the DoD PKI.

We are committed to increasing the security posture of the DoD by providing a seamless security environment supporting Identity Management efforts with the overarching goal of defending and protecting the United States of America.

DoD PKE is the Key to operationalizing PKI.

Visit us on IASE—
http://iase.disa.mil/pki-pke

Send your questions and feedback to—
PKE_Support@disa.mil

PKE Puzzle Corner

Welcome to the inaugural edition of the PKE Puzzle Corner. This is your chance to try your hand at cryptanalysis. We'll be including a new puzzle in each edition of the PKE Quarterly Post. The first person to respond to pke_support@disa.mil with the correct answer will be announced in the next PKE Quarterly Post. Solutions will be posted to the Newsletters section of our web site at http://iase.disa.mil/pki-pke and published in the following edition of the Post. Feel free to drop us a line at pke_support@disa.mil to let us know what you think!

Match the enciphered letter to its corresponding plain text letter to decipher the puzzle.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
																					x				

ahtlzaiarjzafl jdzmtlzarjzafl lfl ptedhajzafl hjzj alztspazo jlh
tlrpoezafl jpt zmt wtrdpazo wtpxartw eqa epfxahtw mfvtxtp
"gdayhals wtrdpazo al" aw zmt qto